

Edge Transitive Ramanujan Graphs and Highly Symmetric LDPC Good Codes

Tali Kaufman *

Alexander Lubotzky †

August 16, 2011

Abstract

We present a symmetric LDPC code with constant rate and constant distance (i.e. good LDPC code) that its constraint space is generated by the orbit of one constant weight constraint under a group action. Our construction provides the first symmetric LDPC good codes. This solves the main open problem raised by Kaufman and Wigderson in [4].

1 Introduction

An (n, k, d) -code is a subspace C of \mathbb{F}_2^X , where $|X| = n$, of dimension k such that the (Hamming) weight of every vector $0 \neq v \in C$ is at least d . A code (or rather a family of codes, when $n \rightarrow \infty$) is called *good* if there exists an $\epsilon > 0$ such that $r(C) = \frac{k}{n}$ (the rate) and $\delta(C) = \frac{d}{n}$ (normalized distance) are both at least ϵ . For a code $C \subseteq \mathbb{F}_2^X$ we denote by C^\perp its dual (i.e. all vectors "orthogonal" to C) and we think of its vectors as the constraints defining the code (i.e. they define linear functionals on \mathbb{F}_2^X whose common set of solutions is C). The code C is called *LDPC* if there exists a set of defining constraints of bounded weight. This bound is called the density of the code.

The code C is said to be *symmetric* (w.r.t. H) if there exists a group H acting *transitively* on X such that the induced action on \mathbb{F}_2^X preserves C . The code C is called *single-orbit symmetric* if in addition there exists $v \in C^\perp$ such that C^\perp is spanned by the orbit $H \cdot v$ (i.e. C is defined by the equation $x \cdot v = 0$ and its translations by H). We say that C is *highly symmetric* if furthermore the vector v can be chosen to have a bounded weight (which, in particular, implies that C is an LDPC). Many of the codes studied in coding theory are symmetric and even single-orbit symmetric (though not necessarily highly-symmetric), e.g., all the cyclic codes (see section 5 below). But, unfortunately cyclic codes do not tend to have the other desired good properties. For example, it is a long standing conjecture that there are no good cyclic codes. An old result of Berman from 1967 [2] proved it for infinitely many code lengths. In [1] Babai, Shpilka and Stefankovic show that cyclic good LDPC codes do not exist.

*Bar-Ilan University, ISRAEL. Email: kaufmant@mit.edu. Research supported in part by the Alon Fellowship.

†Hebrew University, ISRAEL. Email: alexlub@math.huji.ac.il. Research supported in part by the ERC and by the Israel Science Foundation.

In [4] Kaufman and Wigderson initiated the study of highly symmetric LDPC codes. The reader is referred to their paper for motivation. The main question presented there is: **”To what extent can symmetric LDPC codes attain (or even come close to) the coding theory gold standards of linear distance and constant rate?”**

The authors consider the tradeoff between $1/\text{rate}$ and the density in symmetric codes. In the codes known prior to their work, if one was constant then the other was worst possible. They constructed a symmetric code with better tradeoff between $1/\text{rate}$ and the density, namely a symmetric code with constant rate, nearly constant distance, whose density is poly logarithmic in the code length. Thus, their code satisfy some of the gold standards but not all. Moreover, they show that if the group H is abelian or solvable (of bounded derived length) there are no codes satisfying all the desired properties and expressed some skepticism if such codes exist at all.

Our main result is on the optimistic side and give:

Theorem 1 (main). *There exist explicit highly symmetric LDPC good codes.*

So, our codes meet all the ”gold standards” of coding theory. Our code C have:

- Constant rate.
- Constant relative distance.
- Symmetric under a group action H .
- The dual code C^\perp is generated by a single orbit $H \cdot v$.
- The above v can be chosen to have bounded weight. In particular, C is also LDPC.

Our constructions are of Cayley codes, in the framework of [4], but with different groups and different generators. Cayley codes are defined in [4] as follows. Let G be a group of order m and S a symmetric (i.e. $S = S^{-1}$) set of generators of order t . Let $\text{Cay}(G, S)$ be the (right) Cayley graph of G w.r.t. S and E its set of edges. So $|E| = mt/2$. Assume $B \subseteq \mathbb{F}_2^S$ is a linear code. Let $C(G, S, B)$ be the linear subspace of \mathbb{F}_2^E containing all the functions $f : E \rightarrow \mathbb{F}_2$ such that for every $g \in G$ the ”local view” of f at the star of g is in B , i.e. the function $f_g : S \rightarrow \mathbb{F}_2$ given by $f_g(s) := f((g, gs))$ is in B .

In general, Cayley codes are *not* symmetric. The group G acts transitively on the vertices of $\text{Cay}(G, S)$ but not on its edges. The Cayley code is symmetric in the following situation. Let G be a group generated by a symmetric set S (i.e. $S = S^{-1}$) and T a group acting on G (i.e., there exists a homomorphism $\varphi : T \rightarrow \text{Aut}(G)$). Assume that S is an orbit of the action, namely, there exists $\gamma \in G$ such that

$$S = \{\varphi(\alpha)(\gamma) | \alpha \in T\}.$$

In this case one can show, see Section 3, that the semi-direct product group $H = G \rtimes T$ acts on $\text{Cay}(G, S)$ and this action is transitive on the edges.

Now, the group T acts on S and hence on \mathbb{F}_2^S . If the ”small code” B is preserved by T (i.e. B is symmetric w.r.t T), then $H = G \rtimes T$ preserves $C(G, S, B)$. Moreover, if B is single-orbit symmetric

(w.r.t. T), e.g., if T is a cyclic group and B is a cyclic code, then $C(G, S, B)$ is also single-orbit symmetric, and in this case it is also automatically highly symmetric when $|S|$ is bounded. (See Section 3 below).

The following theorem (proved in [4] inspired by [13] and [12]), estimates the parameters of $C = C(G, S, B)$ in terms of those of B and the eigenvalues of the graph $\text{Cay}(G, S)$.

Theorem 2. *Let G, S, T, B as above, with B a code in \mathbb{F}_2^S with rate $r(B)$ and normalized distance $\delta(B)$. Then $C = C(G, S, B)$ is a code with $r(C) \geq 2r(B) - 1$ and $\delta(C) \geq [(\delta(B) - \lambda)/(1 - \lambda)]^2$ where $\lambda = \lambda(\text{Cay}(G, S))$ is the second largest normalized eigenvalue of the Cayley graph $\text{Cay}(G, S)$.*

Corollary 1. *In the notations above; if $r(B) > \frac{1}{2}$ and $\delta(B) > \lambda(\text{Cay}(G, S))$ then $C(G, S, B)$ is a good code. If in addition B is single-orbit symmetric, then so is $C = C(G, S, B)$. Hence, if $|G| \rightarrow \infty$ and $|S|$ is bounded C is highly symmetric.*

The last corollary gives the framework to prove Theorem 1. We will present first edge transitive Cayley graphs $\text{Cay}(G, S)$ (where S is the orbit of a cyclic group T of a fixed size $q + 1$ acting on G , when $|G| \rightarrow \infty$) with $\lambda = \lambda(\text{Cay}(G, S))$ sufficiently small. Secondly, we will find a cyclic code $B \subseteq \mathbb{F}_2^S$ with $r(B) > \frac{1}{2}$ and $\delta(B) > \lambda$. The resulting $C(G, S, B)$ will be highly symmetric and good by Corollary 1. In particular it is also LDPC as it is defined by local equations (in fact the orbit of one equation under the group $H = G \rtimes T$) which touches at most $q + 1$ variables. So, Theorem 1 will be proven once the two goals will be achieved.

For the first mission let us recall that a finite $q + 1$ -regular connected graph is called Ramanujan if for every normalized eigenvalue λ either $|\lambda| = 1$ or $|\lambda| \leq \frac{2\sqrt{q}}{q+1}$. Such graphs were constructed in [7] for every prime p and for every prime power $q = p^\ell$ in [10]. But we will make use of a more recent explicit construction of Ramanujan graphs by Lubotzky, Samuels and Vishne [9] which have some extra symmetry, and in particular are edge transitive.

Theorem 3 (Edge Transitive Ramanujan graphs Theorem). *For a prime power q and for $\alpha \in \mathbb{N}$ such that $q^\alpha > 17$, let $G = \text{PSL}_2(q^\alpha)$ or $G = \text{PGL}_2(q^\alpha)$ and let T be the non split tori of order $q + 1$ in $\text{PGL}_2(q)$. There exists $\gamma \in G$ such that $\text{Cay}(G, S)$ is a $q + 1$ -Ramanujan graph with $S = \{t\gamma t^{-1} | t \in T\}$, $|S| = q + 1$, in particular, the graph $\text{Cay}(G, S)$ is edge-transitive. The element γ will be explicitly defined in section 4. In the case that $G = \text{PGL}_2(q^\alpha)$ the graph $\text{Cay}(G, S)$ is bi-partite.*

The above theorem will give us the desired Cayley graphs. For B we will make a very special choice. Assume now $m \geq 10$, $q = 2^{m+1} - 3$ and assume that q is a prime power. For example, one can take $m = 11$, $q = 4093$ (so q is prime in this case).

Theorem 4 (Good B Theorem). *Let $q \in \mathbb{N}$ be a prime power such that $q + 1 = 2^{m+1} - 2 = 2(2^m - 1)$ for $m \geq 10$. Then there exists an explicit linear binary cyclic code $B \subseteq \mathbb{F}_2^{q+1}$ with $r(B) > \frac{1}{2}$ and $\delta(B) > \frac{2\sqrt{q}}{q+1}$.*

The proof of Theorem 4 will use standard methods of coding theory. The cyclic codes which are natural to be chosen to have the required rate and distance are BCH-codes. However, a little obstacle is caused by the fact that over \mathbb{F}_2 , BCH codes are always of odd length, while for our

construction we need them to be of even length. This is overcome using a trick from [14] (see Section 5 for details).

An interesting number theoretic problem is whether one can find infinitely many q 's suitable for us. I.e. are there infinitely many r 's for which $2^{r+1} - 3$ is a prime (power)? This is a question of the the same style of the famous *Mersenne Primes Problem*; Are there infinitely many primes of the form $2^m - 1$? It seems that with the current knowledge we also do not know the answer even if we replace "primes" with "prime powers". Luckily, we need only one such q and $2^{12} - 3 = 4093$ does the job for us!

2 Notations and Conventions

We start with some basic definitions that are being used throughout this work.

2.1 Group theory definitions

Definition 1 (Action of a group on a set, transitivity). *An action of a group T on a set X is a group homomorphism $\phi : T \rightarrow \text{Sym}(X)$ that sends each element t to a permutation of the elements of X . Let x^t denotes the action of $t \in T$ on $x \in X$. That is, an action should satisfy for every $t, t' \in T, x \in X$*

$$x^{tt'} = (x^{t'})^t$$

The orbit of an element $x \in X$ is

$$x^T = \{x^t | t \in T\}.$$

The action is called transitive if for some (and hence every) $x \in X, x^T = X$.

Definition 2 (Action of a group on a group). *An action of a group T on a group G is a group homomorphism $\phi : T \rightarrow \text{Aut}(G)$. Let $g^t = \phi_t(g)$ denotes the action of $t \in T$ on $g \in G$.*

Definition 3 (Semi-direct product group). *Suppose a group T acts on a group G . The semidirect product $G \rtimes T$ is a group whose elements are pairs (g, t) where $g \in G$ and $t \in T$, and the product is given by:*

$$(g_1, t_1) \cdot (g_2, t_2) = (g_1 \cdot g_2^{t_1}, t_1 \cdot t_2).$$

Note that with the identification of G as a subgroup $\{(g, 1)\}$ of $G \rtimes T$, we have $g^t = tgt^{-1}$ which respects the equality $(g^{t'})^t = g^{tt'}$.

2.2 Graph definitions

Definition 4 (Cayley graph). *Given a group G and a set of generators $S \subset G$ ($S = S^{-1}$), the Cayley graph $\text{Cay}(G, S)$ is a graph, whose vertices are labeled by elements of G . The edges adjacent to $g \in G$ are (g, s) , $s \in S$ and $(g, s) = (gs, s^{-1})$.*

Definition 5 (Edge-transitive graph). *A graph $Y = (V, E)$ is edge-transitive if $\text{Aut}(Y)$ acts transitively on the undirected edges.*

Here is a situation in which the Cayley graph is edge transitive.

Definition 6 (Action of the semi-direct product group). *Let G be a group and $S \subseteq G$ a generating subset with $S = S^{-1}$. Let T be a group acting on G (as group automorphisms) and assume S is invariant under T (i.e. $s^T \subseteq S$, for every $s \in S$). The semi-direct product group $G \rtimes T$ acts on the Cayley graph $\text{Cay}(G, S)$ as graph automorphism as follows. For $(g, t) \in G \rtimes T$, $(g', s) \in G \times S$.*

$$(g', s)^{(g, t)} = (gg^t, s^t)$$

We have the following properties that can be easily verified by direct calculations.

- This is a well defined action, i.e. for $(g_1, t_1), (g_2, t_2) \in G \rtimes T$, $(g', s) \in (G \times S)$,

$$((g', s)^{(g_2, t_2)})^{(g_1, t_1)} = (g', s)^{(g_1, t_1) \cdot (g_2, t_2)}.$$

Note that the undirected edge (g', s) can be also presented as $(g's, s^{-1})$, and indeed:

$$(g's, s^{-1})^{(g, t)} = (g(g's)^t, (s^{-1})^t) = (gg^t s^t, (s^t)^{-1}).$$

which represents the same edge as $(gg^t, s^t) = (g', s)^{(g, t)}$.

- This action is always transitive on the vertices, and if the action of T on S is transitive then the action of $G \rtimes T$ on $\text{Cay}(G, S)$ is edge transitive.
- This action when restricted to G (sitting as a subgroup $\{(g, 1) | g \in G\}$ in $G \rtimes T$) is the usual action of G on $\text{Cay}(G, S)$ by multiplication from the left.

3 Cayley Codes

Definition 7 (Linear code, length, dimension, rate, distance). *Let \mathbb{F} be a field and X a finite set. A linear code $C \subseteq \mathbb{F}^X$ is a linear subspace. The orthogonal space to C is the dual-code C^\perp . The length of the code C is $|X|$. The dimension of the code C is its dimension as a subspace. The rate of C , denoted by $r(C)$, is the dimension of the code divided by its length. The weight of $c \in \mathbb{F}^X$, denoted $w(c)$, is the number of non-zero coordinates in c . The normalized distance of C , denoted $\delta(C)$, is the minimum weight of a non-zero codeword of C , divided by the length of C .*

Definition 8 (Symmetric and Highly Symmetric codes). *Continuing with the notations of Definition 7; We say that a code C is symmetric (or symmetric with respect to G) if there is a group G acting transitively on X such that C is invariant under the induced action of G on \mathbb{F}^X . In such a case C^\perp is also invariant under G (since $v \cdot w^g = v^{g^{-1}} \cdot w$ for every $g \in G$ and $v, w \in \mathbb{F}^X$). We say that C is single-orbit symmetric if there exists $v \in C^\perp$ such that the G -orbit $v^G \subseteq \mathbb{F}^X$ of v spans C^\perp . A code C (or more precisely a family of codes C when $|X| \rightarrow \infty$) is said to be highly-symmetric if C^\perp is spanned by an orbit of v^G where v is of bounded weight.*

So, symmetric C means that "all variables" look the same, and it is also single-orbit symmetric if one equation defines C as a symmetric code. Many of the codes studied classically in coding theory are single-orbit symmetric. For example, all cyclic codes are such (see below and in Section 5). Let us observe that the action of G on X , and hence on \mathbb{F}^X , makes \mathbb{F}^X into an $\mathbb{F}[G]$ -module, where $\mathbb{F}[G]$ denotes the group algebra of G over \mathbb{F} . If C is invariant under G , it simply means that C is an $\mathbb{F}[G]$ -submodule. So, given the transitive action of G on X , symmetric codes in \mathbb{F}^X are the same as $\mathbb{F}[G]$ -submodules. Now, if C is a submodule, so is C^\perp . The symmetric code/submodule C is single-orbit symmetric iff C^\perp is 1-generated submodule (also called cyclic submodule). Note that an $\mathbb{F}[G]$ -module M is 1-generated iff it is isomorphic to a quotient module of $\mathbb{F}[G]$ (as an $\mathbb{F}[G]$ module).

As G acts transitively on X , X can be identified with the coset space G/H of some subgroup H of G and $\mathbb{F}^X = \mathbb{F}^{G/H}$ is a quotient module of $\mathbb{F}^G = \mathbb{F}[G]$, i.e., \mathbb{F}^X is a cyclic module (namely 1-generated). But here a word of warning is needed. In general an $\mathbb{F}[G]$ -submodule of a cyclic $\mathbb{F}[G]$ -module is not necessarily cyclic, which means that symmetric codes are not necessarily single-orbit symmetric.

Here is a well known example. Let \mathbb{F}_p be the field of prime order p and G a finite p -group. Let Δ be the augmentation ideal of $\mathbb{F}_p[G]$, i.e., $\Delta = \text{Ker}(j)$ where $j : \mathbb{F}_p[G] \rightarrow \mathbb{F}_p$ is defined by $j(\sum a_g g) = \sum a_g$ (here $a_g \in \mathbb{F}_p$ and $g \in G$). Then Δ is a submodule (in fact, being the kernel of the homomorphism j , it is even a two sided ideal of the group algebra $\mathbb{F}_p[G]$), and it is well known that its minimal number of generators is equal to $d(G)$, the minimal number of generators of G as a group. Now, when G is not a cyclic group, $d(G) \geq 2$ which shows that if we take $X = G$, \mathbb{F}_p^X has $C = \Delta^\perp$ as a symmetric code which is *not* single-orbit symmetric (since its dual $\Delta = (\Delta^\perp)^\perp$ is not cyclic). For more information about the number of generators of Δ , its powers and general (left) ideals of $\mathbb{F}_p[G]$ (which are exactly its submodules) see [11] - especially Section 5.

On the other hand, if G is a finite cyclic group acting transitively on a set X and \mathbb{F} an arbitrary field, then every submodule of \mathbb{F}^X is cyclic. Indeed \mathbb{F}^X is a quotient of the group algebra $\mathbb{F}[G]$. The last is isomorphic to $\mathbb{F}[t]/(t^n - 1)$ with $n = |G|$, and hence it is a quotient of the polynomial ring $\mathbb{F}[t]$, which is a principle ideal domain and each of its ideals is 1-generated. So, when G is a cyclic group all the codes which are symmetric w.r.t G are automatically single-orbit symmetric. These are the classical so called "cyclic codes" (see more in Section 5).

There is another situation where symmetric codes are automatically single-orbit symmetric; This is when the characteristic of the field \mathbb{F} is prime to the order of G . In this case every $\mathbb{F}[G]$ submodule M of \mathbb{F}^X is also a quotient module (since every $\mathbb{F}[G]$ -module is semi-simple) and as \mathbb{F}^X is 1-generated so is M .

In [4], Kaufman and Wigderson initiated the study of Cayley codes as a method to construct symmetric and highly symmetric codes. We will use this framework in order to construct constant rate, constant distance LDPC codes whose constraint space is generated by one constraint of constant weight.

Definition 9 (Cayley code). *Given a Cayley Graph $\text{Cay}(G, S)$ and a linear code $B \subseteq \mathbb{F}^S$ of length $|S| = t$ define the linear Cayley code $\text{Cay}(G, S, B) \subseteq \mathbb{F}^{|G| \cdot |S|/2}$ as follows. Its coordinates are the $|G| \cdot |S|/2$ undirected edges of the graph $\text{Cay}(G, S)$, namely the pairs $\{(g, s_i), (gs_i, s_i^{-1})\}$, $g \in G, s_i \in S = \{s_1, \dots, s_t\}$. The defining linear constraints are the local constraints of B on the*

edges incident to every vertex, namely

$c \in \text{Cay}(G, S, B)$ iff for every $g \in G$ the following holds:

- **Vertex consistency:** $(c_{\{(g, s_1), (gs_1, s_1^{-1})\}}, \dots, c_{\{(g, s_t), (gs_t, s_t^{-1})\}}) \in B$.

Assume T is a group acting on G and S is an orbit of T , i.e. there exists $\gamma \in G$ s.t. $S = \gamma^T$. Assume further that $S = S^{-1}$. Let $H = G \rtimes T$. As in Definition 6, H acts on $\text{Cay}(G, S)$ and this action is edge transitive. Let now $B \subseteq \mathbb{F}^S$ be a linear code, which is invariant under the action of T (which acts on S and hence on \mathbb{F}^S). It is straight forward now to check that $C = C(G, S, B)$ is invariant under H (see also [4]).

The following proposition now follows easily from the definition.

Proposition 5. *If B is single-orbit symmetric w.r.t T then $C = C(G, S, B)$ is single-orbit symmetric w.r.t $H = G \rtimes T$. Moreover, C^\perp is generated by the orbit of one vector of weight at most $|S|$.*

The second statement follows from the fact that each of the constraints defining C is "local" and touches only the variables associated with the edges around a single vertex.

Before bringing the main theorem of this section, let us recall that if Γ is an r -regular graph of size m , then the eigenvalues of its adjacency matrix are $r = \lambda_0 \geq \lambda_1 \geq \dots \geq \lambda_{m-1} \geq -r$, and we denote $\lambda = \lambda(\Gamma) = \frac{\lambda_1}{r}$ the second normalized eigenvalue of Γ .

The following theorem is proved in [4], Theorem 7. It summarizes Theorem 2 and Corollary 1 from the introduction.

Theorem 6 (Detailed Cayley Codes Theorem). *Let \mathbb{F} be a field. Let G and T be groups, such that T acts on G , $S \subseteq G$ is an orbit for this action. Assume $S = S^{-1}$ and S generates G . The action of T on S induces an action on \mathbb{F}^S . Let $B \subseteq \mathbb{F}^S$ be a linear code invariant under T . Assume that:*

- *$\text{Cay}(G, S)$ is an expander with second normalized eigenvalue λ .*
- *Normalized distance of B is $\delta > \lambda$.*
- *Rate of B is greater than $\frac{1}{2}$ ($r_B > \frac{1}{2}$).*
- *B is T -single-orbit symmetric.*

Then the code $C(G, S, B) \subseteq \mathbb{F}^{G \times S}$ has constant rate at least $2r(B) - 1$ and normalized distance at least $[(\delta - \lambda)/(1 - \lambda)]^2$. It is invariant under the action of the semi-direct product group $H = G \rtimes T$, and it is H -single-orbit symmetric. Moreover, $C(G, S, B)$ is LDPC defined by constraints of weight equal to the one constraint defining B (under the T -action).

4 Edge Transitive Ramanujan Graphs

In this section we prove Theorem 3. This is just a special case of a much more general result in [9] but as the result there is so general, one may find it difficult to see the special case needed here, so we will review it here. In fact, the special case needed here has already been used in [6] for a different reason and was also explained there. We repeat the description for completeness and also in order to give the explicit description of the set of generators S , which amount to give an explicit description of γ in the notations of Theorem 3.

Let \mathbb{F}_q and \mathbb{F}_{q^2} be the fields of order q and q^2 , say $\mathbb{F}_{q^2} = \mathbb{F}_q[\alpha]$ where $\alpha^2 \in \mathbb{F}_q$ is not a square in \mathbb{F}_q . Following the notations of [9], we denote by R the ring $R = \mathbb{F}_q[y, \frac{1}{y}, \frac{1}{1+y}]$, i.e. the subring of the field of rational functions $\mathbb{F}_q(y)$ generated by y , $\frac{1}{1+y}$ and $\frac{1}{y}$. Let $A(R)$ be the four-dimensional R -algebra with a basis $1, \alpha, z$ and αz (i.e. it contains the commutative R -subalgebra $R[\alpha] = \mathbb{F}_{q^2}[y, \frac{1}{y}, \frac{1}{1+y}]$ as a two-dimensional R -module). The multiplication in $A(R)$ is determined by the rules $z\alpha = -\alpha z$ and $z^2 = 1 + y$. As $1 + y$ is central and invertible, z is invertible, in fact, $z^{-1} = \frac{1}{1+y}z$. Denote $b = 1 + z^{-1} \in A(R)$.

Now, $A(R)$ contains $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^2}$. For every $u \in \mathbb{F}_{q^2}^*$, we denote $\tilde{b}_u = ubu^{-1}$. As \mathbb{F}_q^* is in the center of $A(R)$, \tilde{b}_u depends only on the coset of u in $\mathbb{F}_{q^2}^*/\mathbb{F}_q^*$. This gives $\frac{q^2-1}{q-1} = q+1$ elements $\tilde{S} = \{\tilde{b}_u \mid u \in \mathbb{F}_{q^2}^*/\mathbb{F}_q^*\}$ of $A(R)^*$, where for a ring D , we denote by D^* the group of invertible elements.

Let $\tilde{\Gamma}$ be the subgroup of $A(R)^*$ generated by the \tilde{b}_u 's and Γ will be its image in $A(R)^*/R^*$, generated by $S = \{\tilde{b}_u/R^* \mid \tilde{b}_u \in \tilde{S}\}$. For every ideal $I \triangleleft R$, we get a map $\pi_I : A(R)^*/R^* \rightarrow A(R/I)^*/(R/I)^*$ and we denote the intersection $\Gamma \cap \text{Ker}(\pi_I)$ by $\Gamma(I)$ -the congruence subgroup. If $\{0\} \not\cong I \triangleleft R$ is a prime ideal and R/I is a finite field of order q^e , then $A(R/I)$ (a quaternion algebra) is isomorphic to the 2×2 matrix algebra over \mathbb{F}_{q^e} (i.e. to $M_2(\mathbb{F}_{q^e})$) and so $A(R/I)^*/(R/I)^* \simeq PGL_2(q^e)$.

Theorem 6.2 of [9] says that for every $\{0\} \not\cong I \triangleleft R$, the Cayley graph of $\Gamma/\Gamma(I)$ w.r.t. the generators S (or more precisely the images of S in $\Gamma/\Gamma(I)$) is a $(q+1)$ -regular Ramanujan graph. Along the way it is shown there that the set S is symmetric (i.e. $s \in S$ iff $s^{-1} \in S$).

Now if I is a prime ideal of R with $R/I = \mathbb{F}_{q^e}$, then $\Gamma/\Gamma(I)$ is isomorphic to a subgroup of $PGL_2(q^e)$, and Theorem 6.6 of [9] shows that it contains $PSL_2(q^e)$. As the latter is a subgroup of index 2 in the first, $\Gamma/\Gamma(I)$ can be either the first or the second. Moreover, we have enough choices: Theorem 7.1 of [9] ensures that for $q^e > 17$, one can choose I such that $G = PSL_2(q^e)$ or $G = PGL_2(q^e)$ will be obtained. This depends on the image of b : if its image is in $PSL_2(q^e)$ then, as the latter is a normal subgroup of $PGL_2(q^e)$, all its conjugates $\{b_u\}$ are also in $PSL_2(q^e)$ and vice versa. If the image of b is not in $PSL_2(q^e)$, then the resulting graph is bipartite since $PGL_2(q^e)/PSL_2(q^e)$ is a cyclic group of order 2, and as said before, all the generators are outside $PSL_2(q^e)$. As it is explained in Corollary 6.8 of [9], it all depends on the image of $\frac{y}{1+y}$ in $R/I = \mathbb{F}_{q^e}$. If this image is a quadratic residue there, we will get $PSL_2(q^e)$ and, if it is a non-quadratic residue, we get $PGL_2(q^e)$. The discussion in Section 7 of [9] shows that at least when $q^e > 17$, there are sufficiently many irreducible polynomials in $\mathbb{F}_q[y]$ of degree e to have both possibilities.

Finally, let us observe that since $\mathbb{F}_{q^2}^*$ normalizes S , the subgroup $\mathbb{F}_{q^2}^*$ of $A(R)^*$ normalizes $\tilde{\Gamma}$ and hence also $\Gamma(I)$, so $\mathbb{F}_{q^2}^*/\mathbb{F}_q^*$ also acts on $\Gamma/\Gamma(I)$ and the image of S is the orbit of (the image of)

b there. Putting all this information together we see that $\text{Cay}(\Gamma/\Gamma(I), S) = \text{Cay}(G, S)$ is the promised edge transitive Ramanujan graph.

The above description of the results from [9] brings only what is needed for this paper. But let us say a few words about the bigger picture (see also Remark 3.6 of [6], but here we talk only on the case $d = 2$, i.e. trees and not general buildings): The group $A(R)^*/R^*$ is a discrete cocompact lattice in $A(\mathbb{F}_q((y)))^*/\mathbb{F}_q((y))^*$. The latter is isomorphic to $K = \text{PGL}_2(\mathbb{F}_q((y)))$ and it acts on its Bruhat-Tits tree T , which is a $(q+1)$ -regular tree. The element $b \in K$ takes the initial point of the tree (the vertex x_0 corresponding to the lattice $\mathbb{F}_q[[y]]^2$) to a vertex x_1 of distance one from it. The group $\mathbb{F}_{q^2}^*/\mathbb{F}_q^*$ fixes x_0 and acts transitively on the $q+1$ vertices adjacent to x_0 (which are in one to one correspondence with the projective line $\mathbf{P}^1(\mathbb{F}_q)$ on which indeed $\mathbb{F}_{q^2}^*/\mathbb{F}_q^*$ acts transitively!) The group Γ which is generated by the conjugates $\{b_u\}$ acts simply transitively on the vertices of T . This is a special one-dimensional case of a general result of Cartwright and Steger [3]. The Cayley graph of Γ with respect to $\{b_u\}$ can therefore be identified with T and hence the Cayley graph $\text{Cay}(\Gamma/\Gamma(I), \{b_u\})$ is isomorphic to $T/\Gamma(I)$. The fact that the last one is Ramanujan is a deep fact, which follows from the work of Drinfeld (see ([5], [10] and [8])). This is just as in the “old” Ramanujan graphs. The extra symmetry that we have in our case is due to the fact that Γ is normalized by $\mathbb{F}_{q^2}^*/\mathbb{F}_q^*$ which has order $q+1$ and acts transitively on the $q+1$ generators of Γ .

5 Construction of cyclic codes with prescribed parameters

To prove our main theorem, Theorem 1, we will use Theorems 6 and 3, i.e. Cayley codes based on the edge transitive Ramanujan graphs constructed in Theorem 3. What is left is to construct the “small code” B of Theorem 6. This is what we do now. Specifically, we restate and prove a slightly extended version of Theorem 4.

Theorem 7 (Detailed Good B Theorem). *Let $q \in \mathbb{N}$ be a prime power such that $q+1 = 2^{m+1} - 2 = 2(2^m - 1)$ for $m \geq 10$. For any constant $a > 2$, there exists an explicit linear binary cyclic code $B \subseteq \mathbb{F}_2^{q+1}$ with $r(B) \geq \frac{1}{2} + \frac{1}{a} > \frac{1}{2}$ and $\delta(B) > \frac{1}{2 \log(q+1)(a/(a-2))}$. In particular, a can be chosen such that $r(B) > \frac{1}{2}$ and $\delta(B) > \frac{2\sqrt{q}}{q+1}$ (e.g. $a \geq 8$).*

Theorem 7 can be deduced from known results in the literature but the requirement that the cyclic code is of even length (i.e. of length $q+1$ for q being a prime power), makes it less routine. Thus, we provide a self contained proof for the existence of such codes.

In the proof we will also review some of the known properties of cyclic codes. Recall, that a linear code $C \subseteq \mathbb{F}_2^n$ is called *cyclic* if for every $(a_0, a_1, \dots, a_{n-1}) \in C$ also $(a_{n-1}, a_0, a_1, \dots, a_{n-2}) \in C$. To every vector $(a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_2^n$ we associate the polynomial $\sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_2[x]$ and so we can identify \mathbb{F}_2^n with the subspace of polynomials of degree at most $n-1$ in $\mathbb{F}_2[x]$. The latter can be also thought as the elements of the ring $R = \mathbb{F}_2[x]/(x^n - 1)$, i.e., $\mathbb{F}_2[x]$ divided by the ideal generated by $x^n - 1$. Now, if C is a cyclic linear code in \mathbb{F}_2^n , it gives rise to a subspace of R which is invariant under multiplication by x , and hence also by its powers. As C is a subspace, it is invariant under multiplication by any element of R , i.e. C is an ideal in R . Conversely, every ideal of R gives a linear cyclic code in \mathbb{F}_2^n . Now, $\mathbb{F}_2[x]$ is a principle ideal domain and so is R . An ideal C in R is thus

uniquely defined by its generator $h(x)$ which is a polynomial in $\mathbb{F}_2[x]$ which divides $x^n - 1$ (Since in $\mathbb{F}_2[x]$, $(h(x)) \supseteq (x^n - 1)$).

Thus, we have a one to one correspondence between linear cyclic codes, ideals in R and divisors of $x^n - 1$ in $\mathbb{F}_2[x]$. We can also deduce the following proposition

Proposition 8. *In the notation above, $\dim C = n - \deg h(x)$.*

We now move to discuss properties of cyclic codes in \mathbb{F}_2^n for $n = 2^m - 1$ for some $m \in \mathbb{N}$. These are the most studied cyclic codes. Let $E = \mathbb{F}_{2^m}$ be the field of order 2^m . Let $w \in E$ be a primitive element in E . Every $\alpha \in E^* = E - \{0\}$ satisfies $\alpha^n = 1$. In fact, E^* is exactly the set of all the roots of $x^n - 1$. For $\alpha \in E^*$ denote $m_\alpha(x)$ the minimal polynomial of α over \mathbb{F}_2 , i.e., it is the polynomial of minimal degree in $\mathbb{F}_2[x]$ satisfying $m_\alpha(x) = 0$. As $\alpha \in E$, which is extension of degree m , we know that $\deg(m_\alpha(x)) \leq m$. Also, we have $m_\alpha(x) | x^n - 1$ since α is a root of $x^n - 1$, and for every $\alpha \in E^*$, $m_\alpha(x) = m_{\alpha^2}(x)$.

In general, it is not so easy to estimate the distance of the cyclic code C from its generating polynomial $h(x)$. However, this is possible for the following special case that will be used for the proof of Theorem 7. For $1 \leq r \leq n$, denote

$$h_r(x) = \text{l.c.m}\{m_{w^i}(x) | 1 \leq i \leq r\}.$$

Since $m_\alpha(x) | x^n - 1$, also $h_r(x) | x^n - 1$. As $\deg(m_\alpha(x)) \leq m$, $\deg(h_r(x)) \leq rm$. In fact, for every $\alpha \in E^*$, $m_\alpha(x) = m_{\alpha^2}(x)$ and hence $\deg(h_r(x)) \leq rm/2$ (for $r \geq 4$). The polynomial $h_r(x)$ gives rise to an ideal (i.e. to a linear cyclic code) C_r called the $BCH(m, r)$ code. The following proposition provides bounds on the dimension and distance of the $BCH(m, r)$ code.

Proposition 9. *The dimension of the $BCH(m, r)$ code is at least $n - mr/2$ (for $r \geq 4$), and its distance is at least $r + 1$.*

Proof. As the generating polynomial of $BCH(m, r)$ has degree at most $rm/2$ (for $r \geq 4$), we get the bound on the dimension of $BCH(m, r)$ from Proposition 8. For obtaining the bound on the distance of $BCH(m, r)$, note that if the code had a codeword c of weight at most r , the polynomial associated with this codeword $c(x)$ would be of the following form $c(x) = c_1 x^{k_1} + \dots + c_r x^{k_r}$ with $k_1 < k_2 < \dots < k_r$. As $h_r(x) | c(x)$ (since the generating polynomial divides every polynomial that is associated with a codeword of the code) we have that $c(w^i) = 0$ for every $i = 1, \dots, r$. This means

$$\begin{pmatrix} w^{k_1} & w^{k_2} & . & . & . & w^{k_r} \\ w^{2k_1} & w^{2k_2} & . & . & . & w^{2k_r} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ w^{rk_1} & w^{rk_2} & . & . & . & w^{rk_r} \end{pmatrix} \begin{pmatrix} c_1 \\ . \\ . \\ . \\ . \\ c_r \end{pmatrix} = \begin{pmatrix} 0 \\ . \\ . \\ . \\ . \\ 0 \end{pmatrix}$$

But the matrix of coefficients has determinant equal to $\prod_{i=1}^r w^{k_i}$ times the determinant of the Vandermonde matrix of w^1, \dots, w^r . Thus, it is not zero. This implies that $c_1 = \dots = c_r = 0$ \square

We are now ready to prove Theorem 7. By Proposition 9 the $BCH(m, r)$ code for $r \geq 4$ is a linear cyclic code of (odd) length $n = 2^m - 1$, dimension at least $n - mr/2$ and distance at least $r + 1$. Thus, if we take $r = \lfloor \frac{n}{m}(1 - \frac{2}{a}) \rfloor$ for some constant $a > 2$ we get that $BCH(m, r)$ is a cyclic code of dimension at least $n(1/2 + 1/a)$, i.e. with rate at least $1/2 + 1/a$. Moreover, this code has distance at least $\frac{n}{m}(1 - \frac{2}{a})$, i.e. normalized distance at least $\frac{a-2}{ma}$.

However, for our goal we need the final outcome B to be a cyclic linear code of (even) length $q + 1 = 2^{m+1} - 2 = 2(2^m - 1) = 2n$ over \mathbb{F}_2 (where q is a prime power). Using Lemma 10, we can transform the cyclic code $BCH(m, r)$ of length $n = 2^m - 1$, described above, to a cyclic code B of length $q + 1 = 2n$, with the same rate as in $BCH(m, r)$, that is, at least $1/2 + 1/a > 1/2$, and a normalized distance that is half the normalized distance of $BCH(m, r)$. Namely, a normalized distance which is at least $\frac{a-2}{2ma} > \frac{a-2}{2a \log q}$. Now if $m \geq 10$ and $a \geq 8$

$$\delta(B) \geq \frac{a-2}{2ma} > \frac{a-2}{2a \log q} > \frac{2\sqrt{q}}{q+1}.$$

So if we choose $m = 11$ and $q = 2^{m+1} - 3 = 4093$ all the requirements are satisfied and Theorem 1 is proved modulo the following lemma.

Lemma 10 (A transformation of a cyclic code of odd length to a cyclic code of even length). *If there exists a binary cyclic code C of (odd) length $n = 2^m - 1$, dimension k (i.e. rate k/n) and distance d (i.e. a normalized distance of d/n), then there exists a binary cyclic code B of (even) length $2n = 2(2^m - 1)$, dimension $2k$ (i.e. rate k/n) and distance d (i.e. a normalized distance of $d/2n$). Moreover, B is explicitly constructed from C .*

Proof. The following proof is essentially from [14]. We include it here for completeness. Let $n = 2^m - 1$ and $N = 2n$. Define a map $\varphi : \mathbb{F}_2^n \times \mathbb{F}_2^n \rightarrow \mathbb{F}_2^N$ by:

$$\varphi(a_0, a_1, \dots, a_{n-1}, b_0, b_1, \dots, b_{n-1}) = (a_0, b_1, a_2, b_3, \dots, b_{n-2}, a_{n-1}, b_0, a_1, b_2, \dots, a_{n-2}, b_{n-1}).$$

Clearly φ is one to one linear map. Denote $B = \varphi(C \times C)$. Thus, $\dim(B) = 2k$, and so the rate of B , $r(B)$ satisfies $r(B) = 2k/2n = k/n = r(C)$. It is also easy to see that the distance of B is the same as the distance of C i.e. d . This mean that the relative distance of B , $\delta(B) = d/2n = \delta(C)/2$. We only need to show that B is a cyclic code, i.e. that B is an ideal when considered as a subspace of the ring $\mathbb{F}_2[x]/(x^N - 1)$. We claim that B is the ideal generated by $h^2(x)$ where $h(x)$ is the generator of C as an ideal of $\mathbb{F}_2[x]/(x^n - 1)$. Note first that $x^N - 1 = x^{2n} - 1 = (x^n - 1)(x^n + 1) = (x^n - 1)^2$ and hence $h^2(x) | x^N - 1$, since $h(x) | x^n - 1$. Also, note that $\dim(B) = 2\dim(C) = 2(n - \deg(h(x))) = N - \deg(h^2(x))$. Thus, it suffices to show that every element of C is divided by $h^2(x)$. For $a(x), b(x) \in C$ write

$$\begin{aligned} a(x) &= a_0 + a_1x + \dots + a_{n-1}x^{n-1} \\ &= (a_0 + a_2x^2 + \dots + a_{n-1}x^{n-1}) + x(a_1 + a_3x^2 + \dots + a_{n-2}x^{n-3}) \\ &= a_{\text{even}}(x^2) + xa_{\text{odd}}(x^2) \end{aligned}$$

Note that n is odd. Similarly $b(x) = b_{\text{even}}(x^2) + xb_{\text{odd}}(x^2)$. Then $w(x) = \varphi(a(x), b(x))$ can be written as

$$\begin{aligned}
w(x) &= (a_{\text{even}}(x^2) + x^{n+1}a_{\text{odd}}(x^2)) + (xb_{\text{odd}}(x^2) + x^n b_{\text{even}}(x^2)) \\
&= (a(x) + x(x^n + 1)a_{\text{odd}}(x^2)) + (b(x) + (x^n + 1)b_{\text{even}}(x^2))
\end{aligned}$$

Both terms $F(x) = (a(x) + x(x^n + 1)a_{\text{odd}}(x^2))$ and $G(x) = (b(x) + (x^n + 1)b_{\text{even}}(x^2))$ are divisible by $h(x)$, since $h(x)$ divides $a(x), b(x)$ and $x^n - 1 = x^n + 1$. Also we have that $F(x) = (a(x) + x(x^n + 1)a_{\text{odd}}(x^2)) = (a_{\text{even}}(x^2) + x^{n+1}a_{\text{odd}}(x^2))$ contains only even powers of x , and $G(x) = (b(x) + (x^n + 1)b_{\text{even}}(x^2)) = (xb_{\text{odd}}(x^2) + x^n b_{\text{even}}(x^2))$ contains only odd powers of x . This implies that both terms are actually divisible by $h^2(x)$. Indeed, $F(x) = f^2(x)$ for some polynomial $f(x) \in \mathbb{F}_2[x]$ and $G(x) = xg^2(x)$ for some polynomial $g(x) \in \mathbb{F}_2[x]$. Now, $h(x)|F(x)$ and $h(x)|G(x)$, also, 0 is not a root of $h(x)$ and all the roots of $h(x)$ are of multiplicity one (here we use the fact that n is odd). Thus, we deduce that $h(x)$ divides $f(x)$ and $g(x)$, which implies that $h^2(x)$ divides $F(x)$ and $G(x)$ and hence $w(x)$.

□

In summary we have proved:

Theorem 11 (A highly symmetric LDPC good code). *Let $q = 4093$, $\alpha \in \mathbb{N}$, $G = PSL_2(q^\alpha)$ or $G = PGL_2(q^\alpha)$, T the group $T = \mathbb{F}_{q^2}^*/\mathbb{F}_q^* \leq PGL_2(q)$, $\gamma \in G$ as in Section 4, $S = \{t\gamma t^{-1} | t \in T\}$. Let $B \in \mathbb{F}^S$ be the code defined in Section 5, with $a \geq 8$. Then $C(G, S, B)$ is a linear code of rate at least $\frac{2}{a}$, normalized distance at least*

$$\left(\frac{\frac{a-2}{2a \log q} - \frac{2\sqrt{q}}{q+1}}{1 - \frac{2\sqrt{q}}{q+1}} \right)^2.$$

The code is symmetric with respect to the action of the semi direct product group $G \rtimes T$, and C^\perp is generated by the orbit of a single constraint of weight at most $q + 1$. In particular, for $\alpha \rightarrow \infty$, this is a family of highly symmetric LDPC good codes.

References

- [1] L. Babai, A. Shpilka and D. Stefankovic, *Locally testable cyclic codes*, IEEE Transactions on Information Theory, Vol 51, No 8, 2849–2858. 2005.
- [2] S. D. Berman. *Semisimple Cyclic and Abelian Codes*. Cybernetics 3, 21-30, 1967.
- [3] D. I. Cartwright and T. Steger. *A family of \tilde{A}_n -groups*, Israel J. Math, Vol 103, 125–140, 1998.
- [4] T. Kaufman and A. Wigderson *Symmetric LDPC and local Testing*, Innovations in Computer Science, 406–421, 2010.
- [5] A. Lubotzky *Discrete groups, expanding graphs and invariant measures*. With an appendix by Jonathan D. Rogawski. Reprint of the 1994 edition, Modern Birkhauser Classics, Birkhauser Verlag, Basel, iii + 192, 2010.

- [6] A. Lubotzky *Simple groups of Lie type as expanders*, J. of the European Math. Soc., to appear.
- [7] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, Combinatorica 8, no. 3, 261–277, 1988.
- [8] A. Lubotzky, B. Samuels and U. Vishne, *Ramanujan complexes of type \tilde{A}_d* Israel J. Math. Vol 149, 267–299, 2005.
- [9] A. Lubotzky, B. Samuels and U. Vishne, *Explicit constructions of Ramanujan complexes of type \tilde{A}_d* , European J. Combin. 26 , no. 6, 965–993, 2005.
- [10] M. Morgenstern, *Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q* , Journal of Combinatorial Theory, Series B 62, 44–62, 1994.
- [11] A. Shalev, *Subgroups, nilpotency indices, and the number of generators of ideals in p -group algebras*, J. Algebra 129, no. 2, 412–438, 1990.
- [12] M. Sipser and D. A. Spielman, *Expander codes*, IEEE Transactions on Information Theory, Vol 42, No 6, 1710–1722, 1996.
- [13] R. M. Tanner, *A recursive approach to low complexity codes*, IEEE Transactions on Information Theory, 27(5):533–547, 1981.
- [14] J. H. van Lint *Repeated-Root Cyclic Codes* IEEE Transactions on Information Theory, Vol 37, No 2, 343–345, 1991.